Kraemer

HIRDLS

TC-LOC-212

HIGH RESOLUTION DYNAMICS LIMB SOUNDER

Originator: Ron Baraze

Date: 14/Jul/97

HIRDLS Autonomous Fault Management

Description/Summary/Contents:

This document describes the actions which will be taken autonomously by the HIRDLS instrument in the event of a detected hardware or software fault.

Keywords: fault, error handling

Purpose of this Document: fault management
(20 char max.)

Reviewed/Approved by: Date (yy-mm-dd):			

Lockheed Palo Alto Research Laboratory
Lockheed Research and Development Division
3251 Hanover Street
Palo Alto, California 94304-1191
U.S.A.

EOS

1. INTRODUCTION

1.1 Purpose and Objective

The purpose of this document is to identify and describe any fault conditions in the operation of the HIRDLS instrument which require immediate instrument or spacecraft action to either protect the safety of the instrument, or to handle conditions that would be difficult to correct from the ground. Each condition is described, along with the reasons why an autonomous action is required, and the action to be taken.

1.2 Organization of Document

The organization of this document is as follows:

- Section 2 Related Documentation
- Section 3 Autonomous Philosophy
- Section 4 HIRDLS Instrument Autonomous Actions

2. RELATED DOCUMENTATION

2.1 Parent Documents

This document is not rolled-out from any higher level document.

2.2 HIRDLS Related Documents

GSFC 422-11-12-01	EOS General Instrument Requirements Document
SP-HIR-13M	Instrument Technical Specification for HIRDLS
CDRL 303	Command and Telemetry Handbook

3. AUTONOMOUS PHILOSOPHY

3.1 Ground vs. Autonomous

Under most conditions, a fault in the HIRDLS instrument will only be detectable by ground based software, which would result in a decision to send one or more commands to diagnose and correct the fault. The only faults which require an autonomous action to be taken by the HIRDLS instrument or the CHEM spacecraft are those which either cannot wait for 24 hours for a corrective action, or those faults which require special actions before the instrument can continue operating.

The first type of faults are actions which will cause damage to the instrument within 24 hours of being detected. This is an estimated time from a detected fault being received and processed by the flight operations controller to a determination of the corrective actions to be transmitted to the spacecraft.[1] These include detected failures of a subsystem's power converters, mechanical failures where continued actions may cause permanent damage, protecting the thermal condition of the warm filters and the detectors, or communication failures which block any of the above conditions from being detected. This also includes a failure of communication between the instrument and the spacecraft.

The second type of faults are those which are either easily correctable, retries on communication errors, or safing procedures which require ground intervention before continuing. These include memory error detection and correction (EDAC) faults, automatic retries in the event of a single event upset (SEU), non-critical communication failures, watchdog timeouts, or initialization faults.

All other types of faults not listed in the following sections must be handled by ground commands. These would include science data errors, box temperatures, calibration errors, command errors, and any other conditions determined to be a instrument fault.

Due to its nature, the Science Algorithm Implementation Language (SAIL) will not be used for fault management. See the section below on Overriding Actions for additional information.

3.2 Actions to be taken

Autonomous corrections are intended to protect the instrument and allow for corrective actions by the ground. Continuation of science data processing is not an important consideration in the corrective actions unless no harm can possibly occur by continuing. Hence, other than simple retry or reinitialize actions, only shutdown actions will be taken, leaving the ground operations to either reactivate or switch to redundant systems.

In all cases, the simplest action to protect the instrument will be taken. Some types of errors will activate more than one fault management action. For example, if communication between the IPU and TEU is lost, three separate fault management actions may be activated: the IPU will try to reinitialize its side, the TEU will try to reinitialize its side, and the mirror will be safed if no commands are received within a specified amount of time.

3.3 Spacecraft Actions

For most of the listed faults, the instrument can handle its own recovery. The exceptions to this are if the fault is in the IPU or PCU power systems, or a 1553 error occurs which cannot be corrected through reinitialization. If the HIRDLS instrument does not communicate to the spacecraft, the spacecraft must attempt to fix the problem from its end. After 120 seconds, if communication cannot be reestablished, the spacecraft should power down the quiet and noisy busses (QBA, QBB, NBA, NBB) for the HIRDLS instrument. This will have given the instrument enough time to have noticed the problem and have completed its own safing procedures. For non-1553 errors, the HIRDLS instrument will use the service request (SR) and subsystem fail (SSF) bits of the 1553 status word to trigger actions. These spacecraft actions should be in macros so they can be changed by ground command.

3.4 Overriding Actions

The default actions listed in the next section can be changed or eliminated by ground command. On each power up, all fault conditions are enabled with a default set of initialization parameters. Commands are available to disable and re-enable a condition, as well as changing the parameters for initialization. For some of the fault conditions, if a condition or action needs to be replaced which is not covered by the parameters, the default condition can be disabled and a SAIL task can be used for the fault management. Other fault conditions would require a new program patch to be uploaded, but this practice is strongly discouraged.

4. HIRDLS INSTRUMENT AUTONOMOUS ACTIONS

The following is the list of autonomous fault conditions which will be handled by the HIRDLS instrument. Each fault is listed with the following fields:

Condition: *The condition lists the type of fault and how it can be recognized.*
Cause: *A cause is a list of likely reasons for the fault to have occurred. This is informational only, and will not be a comprehensive list, nor will this list be sorted in any fashion.*
Action: *This is the action to be taken, as well as the subsystem to take the action. This will also list what parameters are required for the action (if any).*
Reason: *The reasoning behind the action are listed, along with information on why stronger or weaker actions were not used.*

Condition: IPU fails to communicate with the spacecraft for 120 seconds after power is applied.
Cause: Corruption of IPU startup ROM, bad voltage converter, SEU error, IPU hardware failure, 1553 failure.
Action: After 120 seconds of no communication, the spacecraft should power down the quiet and noisy busses (QBA, QBB, NBA, and NBB) for HIRDLS using a spacecraft macro sequence.
Reason: Without 1553 communication, no data is available to determine what caused the failure, and commands cannot be sent. The ground should either retry on the failed side, or power up the redundant system.

Condition: The checksum of the IPU program in EEPROM fails to match its stored value during the IPU boot sequence.
Cause: SEU corruption of data while transferring to RAM, permanent multiple-bit failure in EEPROM which cannot be corrected by EDAC, EDAC unit failure.
Action: Retry the readout of the failed section once, and then force the IPU into boot hold to wait for ground corrective action. If the retry succeeded, mark the attempt in the next telemetry status packet.
Reason: If the failure was in the transfer to RAM, one retry should correct be problem. Any permanent failure in EEPROM can be fixed by either uploading a new program from the ground, or maybe by loading a compressed backup copy out of another location of EEPROM.

Condition: The IPU watchdog bites (timed out).

Cause: SEU hit in R6000 processor or LIO, interrupt lockout, power glitch, infinite EDAC loop, damaged watchdog circuitry.

Action: Power down the DSS. If active, unlatched and out of position, safe the scanner mirror and sunshield door. SAIL commanding of the sunshield and scanner mirror will be disabled. Reboot the IPU after the safing sequence completes, but freeze in the boot hold state so the IPU memory contents are preserved.

need to check this

Reason: As long as the operating system and its interrupts are functional, and the command and telemetry system is working, the watchdog should be tickled (reset) often enough that it will not reach zero. As the event or series of events which caused the watchdog to time out cannot be determined on board, the memory contents will be preserved so the ground can determine what happened and take any corrective actions needed.

Condition: IPU or TEU single bit corrected EDAC error occurs.

Cause: SEU event, EDAC unit failure

Action: For IPU or TEU RAM, the corrected value will be written back to avoid a repeat of the same error next time the location is accessed, and the total number of corrections will be marked in the next telemetry status packet. For IPU EEPROM errors, the new value will be used but not rewritten to EEPROM, and the error will be marked in the next telemetry packet with its location.

Reason: RAM single bit errors will be an infrequent but expected occurrence, and hence the use of the EDAC to correct these types of errors. EEPROM errors may occur, but only ground commanding will be allowed to change EEPROM contents.

Condition: IPU or TEU double bit detected (uncorrected) EDAC error occurs.

Cause: Multiple overlapping SEU events, permanent RAM or EEPROM bit failures, EDAC unit failure.

Action: Reboot the processor and remain in the boot hold state for corrective action to be taken by the ground. For the TEU, automatic boot from the IPU will be disabled.

Reason: Multiple bit errors cannot be properly corrected, and continued execution with faulty code and/or data could produce harmful results. Corrective action from the ground is required to determine what caused the failure, and if the failure is a permanent RAM or EEPROM defect, a software patch may be required to avoid using the memory in the future. Note that the instrument cannot be automatically safed, since the double bit errors may have corrupted the safing sequences.

Condition: 1553 HIRDLS to Spacecraft communication failed (no data received or transmitted) for at least 1 second.

Cause: Spacecraft bus controller (BC) failure, HIRDLS remote terminal (RT) failure, built-in-test failed to complete, SEU corruption of 1553 vector table or registers

Action: The IPU will reset and reinitialize the 1553 RT once every two seconds for a maximum of 30 seconds. If communication is not reestablished within 1 second of a reset, the IPU will activate the system request (SR) bit of the 1553 status word. If the spacecraft receives the SR bit, a reset RTR mode code should be sent to HIRDLS using a spacecraft macro sequence. If communication cannot be reestablished within the 30 seconds, the subsystem fail (SSF) bit will be activated, and the DSS will be powered off. If active, unlatched and out of position, the scanner mirror and sunshield door will be safed. SAIL commanding of the sunshield and scanner mirror will be disabled. After 120 seconds of either no communication or receiving the SSF bit, the spacecraft should power down the quiet and noisy busses (QBA, QBB, NBA, and NBB) for HIRDLS using a spacecraft macro sequence.

Reason: If a 1553 failure cannot be corrected by either the instrument or the spacecraft, no further actions are possible. Without communication, the health and safety of the instrument cannot be determined by the spacecraft or ground, and hence the power should be turned off.

Condition: TEU fails to bootup and communicate with the IPU within 10 seconds of power turn on, or communication with the TEU during normal operations is lost for at least 1 second.

Cause: Corruption of IPU startup ROM, bad voltage converter, SEU error, TEU hardware failure, QHSS failure, broken harness wire.

Action: Each second, the IPU and the TEU will reinitialize each failed QHSS link to establish communications. After 10 seconds with no engineering data link or 60 seconds with no command or science data link, the IPU will command the TEU to be powered off. After 30 seconds with no command link, the TEU will abort the current scan sequence and safe the scanner mirror.

Reason: If no engineering data link is available, the health and safety of the TEU cannot be determined. If no command or science data link is available, no further normal or corrective actions can be taken, nor can science data collection continue. The ground will need to determine what caused the failure and either power up the primary or redundant unit.

Condition: The checksum of the TEU program in the IPU EEPROM fails to match its stored value during the TEU boot sequence.

Cause: SEU corruption of data while transferring to RAM, permanent multiple-bit failure in EEPROM which cannot be corrected by EDAC, EDAC unit failure.

Action: Retry the readout of the failed section once; if unsuccessful, hold off TEU boot until the ground can take corrective action. If the retry succeeded, mark the attempt in the next telemetry status packet.

Reason: If the failure was in the transfer to RAM, one retry should correct be problem. Any permanent failure in EEPROM can be fixed by either uploading a new program from the ground, or maybe by loading a compressed backup copy out of another location of EEPROM.

Condition: The checksum of a TEU bootload packet fails to match the sent value.

Cause: QHSS error, QHSS RAM failure, SEU error, internal bus error, EDAC error (all of these could be in the IPU or TEU).

Action: Rewrite the packet into the IPU QHSS RAM and retransmit up to two more times. If the failure persists, hold off TEU boot until the ground can take corrective action. If the retry succeeded, mark the attempt in the next telemetry status packet.

Reason: A SEU error anywhere in either the IPU or TEU should be corrected with the retries. Anything else will require ground diagnostics to determine where the problem occurred. The TEU application code will not be executed unless all packets have been checksum verified.

Condition: The TEU watchdog bites (timed out).

Cause: SEU hit in R6000 processor or LIO, interrupt lockout, power glitch, infinite EDAC loop, damaged watchdog circuitry.

Action: Power down the drive motors. Reboot the TEU, but freeze in the boot hold state so the memory contents are preserved. The automatic boot from the IPU will be disabled. The IPU should safe the sunshield door once the TEU reboot is detected as the scanner mirror position cannot be determined.

Reason: As long as the operating system and its interrupts are functional, and the command and telemetry system is working, the watchdog should be tickled (reset) often enough that it will not reach zero. As the event or series of events which caused the watchdog to time out cannot be determined on board, the memory contents will be preserved so the ground can determine what happened and take any corrective actions needed. Note that the scanner mirror

Condition: A non-switchable low-voltage converter in IPU or PCU reports an overcurrent, undervoltage, or overvoltage condition.

Cause: Bad voltage converter, bad sensor reading.

Action: A fault will not be flagged until at least three consecutive readouts of the sensor are in error. The IPU will activate the subsystem fail (SSF) bit of the 1553 status word, and power off the DSS. If active, unlatched and out of position, the scanner mirror and sunshield door will be safed. After 120 seconds of receiving the SSF bit, the spacecraft should power down the quiet and noisy busses (QBA, QBB, NBA, and NBB) for HIRDLS using a spacecraft macro sequence. If the sensor produces three consecutive valid readouts, the SSF bit will be cleared and the spacecraft should abort the pending shutdown, but resumption of data collection will need to be restarted by the ground.

Reason: Non-switchable power converters can only be corrected by ground command by switching to the redundant set. Readout failures must be determined by the ground and a sequence of commands to ignore the bad sensor(s) can be sent. Taking no action may damage the instrument, but some amount time is needed to get the readings to the ground and to accept corrective commands.

Condition: A switchable low-voltage converter in any subsystem reports an overcurrent, undervoltage, or overvoltage condition.

Cause: Bad voltage converter, bad sensor reading.

Action: A fault will not be flagged until at least three consecutive readouts of the sensor are in error. Execute a safing sequence if one exists for the affected subsystem, but allow no more than 60 seconds for the sequence to attempt completion. Power off the subsystem at the completion of the safing sequence or 60 seconds, whichever is shorter. For systems without safing sequences, wait for 10 seconds to collect diagnostic data for ground diagnosis, then power down. If the sensor produces three consecutive valid readouts prior to the power down, the shutdown will be aborted.

Reason: Switchable power converters should be turned off to avoid possible instrument damage, and enough data is taken so the ground can determine if the reading was due to a bad converter or a sensor failure.

Condition: The sun sensors on the sunshield door report multiple hits which the voting logic determines to be sunlight.

Cause: Light on the sun sensors, numerous sun sensor failures.

Action: A fault will not be flagged until at least three consecutive readouts of the sensor are in error. If the fault persists, power down the DSS, and, if active, unlatched and out of position, safe the scanner mirror and sunshield door. SAIL commanding of the sunshield and scanner mirror will be disabled.

Reason: Light on the sun sensors may cause sunlight to be reflected onto the warm filters and detectors, which can cause delamination of the filters and other permanent damage within a few seconds.

Condition: The scanner mirror fails to move in azimuth or elevation when commanded.

Cause: Drive motor failure, software error, position readout error.

Action: If no movement occurs within 5 seconds, a fault condition exists. For azimuth, disable power to the failed motor. For elevation, disable motor 1 first and wait another 5 seconds. If no movement occurs, then also disable motor 2. Scanning in the other axis can continue.

Reason: The motors are disabled to prevent overheating and burnout. The ground can take corrective action by using the redundant windings or selectively powering motors to determine the cause of the fault.

Condition: The sunshield or cold reference door motor fails to move when commanded, or reaches an overcurrent or above maximum temperature condition.

Cause: Door not unlatched, door at stop, drive motor failure, position readout failure, latching mechanism failure, software error.

Action: If the door fails to move for 10 seconds, or three consecutive readouts of current or temperature show a fault, the motor will be shutdown. If the fault is in the sunshield motor, SAIL commanding of the sunshield will be disabled.

Reason: The motors are disabled to prevent overheating and burnout. The ground can take corrective action by retrying the action or using the redundant windings.

Condition: After reaching its operating speed, the chopper has any of the following faults: a) the frequency of the chopper cycles deviates from its commanded rate by more than 1 millisecond for three cycles as measured by the IPU HIRDLS clock; b) the frequency of the chopper rotation signal varies by more than 10 milliseconds for three rotations as measured by the IPU HIRDLS clock; c) the chopper fails to provide either the cycle or the rotation signal to the IPU or TEU for at least 100 milliseconds; d) the chopper current readout shows an overcurrent condition for three consecutive readouts; and/or e) the chopper exceeds its maximum temperature setpoint for three consecutive readouts.

Cause: Chopper hardware failure, IPU reference signal error, broken wire, ramp-up circuit failure, HIRDLS clock failure, temperature or current sensor failure, SEU error.

Action: For frequency failures (a) and/or (b), the IPU will rewrite the reference signal frequency register with the original commanded value. As long as none of the other conditions (c), (d), or (e) occur, the chopper will be given 10 seconds to return to normal speed. If either frequency is still out of range after 10 seconds, or any of the conditions (c), (d), or (e) occur, the chopper will be shut down as described below. If the TEU does not receive either signal for 100 milliseconds, it will switch to its internal reference clock, but take no other action unless commanded. If the IPU does not receive a signal for 100 milliseconds, detects a overcurrent or above temperature condition, or is shut down due to the frequency failures described above, the following actions will occur: (a) the IPU will switch to its internal sync clock; (b) the TEU will be commanded to switch to its internal sync clock; (c) the IPU reference signal to the chopper will be disabled; (d) the power and/or driver signals to the chopper motor will be disabled.

Reason: The chopper is a single-point critical hardware device for HIRDLS. Any error other than simple frequency errors must be detected and corrected by ground commanding to protect the chopper from permanent damage.

Condition: The blackbody exceeds its maximum temperature setpoint.

Cause: Temperature controller failure, SEU error, software error.

Action: All blackbody heaters will be disabled, and SAIL commanding of the blackbody temperature will be disabled.

Reason: The blackbody can be damaged by excessive heat, and the ground can determine what caused the failure and take corrective action.

Condition: The TEU has not received a new scan table command within 30 seconds of completing the execution of the previous table.

Cause: SAIL scanner task suspended, killed, or in error, QHSS failure, IPU reset, software error.

Action: The mirror will be moved to its safe position after 30 seconds, and the QHSS will be reinitialized.

Reason: The IPU should always be commanding the scanner mirror. To protect the filters and detectors, the scanner mirror will be moved to its safe position since the state of the sunshield door is unknown to the TEU.

Condition: The CSS cold tip sensor or the DSS temperature sensors are above the maximum commanded setpoint.

Cause: High temperature, sensor failure.

Action: If three consecutive readouts of any sensor show an above temperature condition, the DSS will be powered down until three consecutive readouts show a temperature below the low commanded setpoint on all sensors. Once all sensors agree, the DSS will be powered up again.

Reason: The DSS may be damaged if powered above its operating temperature.

Condition: If powered, the QHSS data link from the SPU to IPU fails to provide data during a chopper revolution.

Cause: SPU failure, QHSS error, chopper signal to SPU failure, broken wire.

Action: If data is not received within a chopper revolution, the IPU will reinitialize its QHSS link. If data has not been received for 8 chopper revolutions, the SPU will be powered down for 5 seconds, then powered back on. If no data is received within 1 second, the SPU will be powered off until commanded by the ground.

Reason: The SPU is designed to provide data once per chopper revolution. If the QHSS link is in error, either the reinitialization or the power up should clear the error. Any other condition must be diagnosed and corrected from the ground.

Condition: A 422 link between the IPU and either the PSS, CSS, or GSS fails.

Cause: 422 error, broken wire, SEU error.

Action: Both sides should reinitialize the 422 link at least once per second until communication is reestablished. If another fault occurs which would require the PSS link to be active, the IPU can request an instrument shutdown by activating the subsystem fail (SSF) bit of the 1553 status word as described in the non-switchable overcurrent fault condition.

Reason: These faults would cause a loss of data, but should not cause a critical failure.

Condition: A loss of communication occurs between the TEU and EEA.
Cause: Communication error, broken wire, SEU error.
Action: Both sides should reinitialize the link once per second for at least 5 seconds. If the condition persists, the mirror should be safed and the EEA will be powered down.
Reason: Any non communication related failure of the EEA will need to be diagnosed from the ground.

Condition: A subsystem has an internal loss of communication, such as an R6000 AMBI bus failure.
Cause: SEU error, hardware failure.
Action: The internal bus should be reinitialized until the system is functional. Note that persistent failures may cause another fault action to be taken.
Reason: Internal errors will usually involve a loss of communication with external interfaces and cannot be corrected by command. If the internal error does not cause another fault, the ground will need to switch off the affected subsystem.